



CVE-2017-3305

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3305
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 19:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that a

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All

References

Reference
MySQL Multiple Flaws Let Remote Authenticated and Local Users Modify Data, Remote and Local Users Deny Service, and Remote Authent
Debian -- Security Information -- DSA-3834-1 mysql-5.5
Oracle Critical Patch Update - April 2017
Red Hat Customer Portal
oss-security - CVE-2017-3305 - The Riddle vulnerability in MySQL client (public disclosure)
MySQL CVE-2017-3305 Man in the Middle Security Bypass Vulnerability
Riddle in the middle
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)